ABSTRACT OF THE DISCLOSURE

The invention concerns the bit error resilience of an IP protocol stack based on a secure link layer, in which packet flows are header compressed according to a suitable header compression standard. According to the invention, by analyzing each packet at the link layer it can be determined whether the packet is a full header packet, in which case the link layer checksum evaluation is used as normal for discarding faulty full header packets, or a header compressed packet in which case the link layer checksum evaluation is ignored and the packet is propagated upwards in the protocol stack. This solution not only opens up for more intelligent higher-level handling of faulty header compressed packets, but also solves the problem of properly protecting full header packets at the link layer. In order to compensate for ignoring the link layer checksum evaluation for header compressed packets, header protection is introduced at the header compression level of the link layer by using one or more local checksums. The invention is particularly applicable to delay-sensitive real-time data such as compressed voice or video.

(Fig. 5)